1. OBJECTIVE

(a) This manual provides a management framework that can be used to reduce the risk of cyber incidents that could affect the safety or security of the ship, its crew, passengers or cargo.

(b) It also describes the measures that may be implemented alone or in combination with others to ensure that the Electronic Computerized system on board vessel remain protected and safe in the event of a cyber-security threat or incident, as well as to provide possible means to recover functionality of the equipment in the event of an incident.

(c) This manual also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems and building resilience and recovery in the event of a compromise.

2. SUMMARY

(a) Modern computerized equipment serves many useful and often indispensable roles / services on board vessel in daily activities. Maintaining Communications with shore, regular reporting of positions, use of Electronic charts for navigation and their updates are not only vital for daily ship operations, but also are a pre-requisite for safe operation of ships and to prevent accidents.

(b) Ships are becoming increasingly complex and dependent on the extensive use of digital and communications technologies throughout their operational life. Therefore, the safety and protection of the on-board computerized equipment is of paramount importance and such equipment should be handled carefully keeping its importance in mind.

(c) Company provided hardware and software may only be utilized for business purposes relating to the Company. No personal use of Company assets is allowed. This includes the Company official email system and Internet access.

(d) The Company provided onboard Internet access is always to be used in a responsible manner. Accessing of suspicious websites are prohibited.

(e) Any communications related to the vessel or company operations and events to third parties or personal email, Social Media or Networking Apps or Websites is prohibited.

(f) The Company reserves the right to withdraw access if & when needed.

3. RESPONSIBILITY

(a) The Master is responsible for the following:

(i) To manage and coordinate the cyber security of a ship in accordance with Company advice on such matters. Cyber Security is constantly changing as newer attacks and defenses become available.

(ii) The Master will disseminate cybersecurity information received to crew or relevant persons and to emphasize that it is the responsibility of every individual on board and

ashore to zealously safeguard the Company's information, digital assets and infrastructure, thus preventing them from being compromised.

(iii) The Master may delegate some of the above responsibilities to another responsible officer but maintains the overall responsibility.

(iv) To keep custody and inventory of any software in USB, CD, etc., software licenses, dongles, drivers, restricted or special IT equipment, etc.

(b) The office IT Manager is responsible for the following:

(i) To keep the Master updated on latest threats and defenses available to mitigate the risk of a cyber security incident. Such information should be shared with the on-board staff as applicable.

(ii) The IT Manager will review and approve the vessel's digital infrastructure installation and evaluate any changes required to the infrastructure and procedures to improve protection against cyber security incidents and resilience of on-board digital assets and services.

(iii) The IT Manager may monitor the on-board IT infrastructure and take any actions needed to protect them in order to maintain or recover their operational status.

(c) The Company reserves the right to monitor the electronic and IT infrastructure, including any information created, used, stored or transmitted by any persons on vessel computer systems and networks. This may include monitoring of usage patterns, websites accessed, emails to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the with company policy. Notwithstanding the above, it is not company policy or intent to continuously monitor all computers usage by vessels.

4. REPORTING

(a) The Master shall report any cybersecurity incidents or threats to the CSO and IT team as soon as practically possible in order seek advice on mitigation measures and alternatives to restore lost functionality earliest possible, using whatever means of communication is available.

(b) Troubles with or malfunction of the IT equipment, systems or infrastructure should be reported earliest to the vessel PIC and IT team (itsupport@mmstokyo.co.jp) via any available working communication for further troubleshooting or support as required.

(c) Further CCD-17-00 Ship Specific – Emergency Contact Numbers shall be referred to, posted on ships, if so required.

5. CONSEQUENCES

(a) The approach to providing effective cybersecurity methods and measures lies in viewing cybersecurity as an integral part of the Risk Assessment of the vessel operations.

(b) If Cybersecurity threats or measures designed to protect and maintain the IT system onboard are ignored, they may cause any or many of the below:

(i) Catastrophic failure leading to unavailability of the equipment function
(ii) Erroneous computations that may affect its accuracy or reliability
(iii) Cause accidents, loss of life, vessel or cargo or cause pollution
(iv) Loss or theft of vital, personal or commercial data
(v) Data loss leading to incidents, loss of business and reputation
(vi) May lead to litigation and / or penalties

(c) Some of the the above scenarios have the capability to affect not only a single ship, but may affect the entire fleet and shore operations, severely affecting the business and also the ability to provide timely and much needed support to the fleet vessels.

(d) All Ship-staff and shore personnel involved in operating any digital assets (computers, computerized equipment) which are subject to cyber-security threats should understand cyber security and be aware of this subject, in order to provide adequate protection, prevention, mitigation and resilience against cyber security events.

6. THREATS

6.1. IDENTIFICATION OF SENSITIVE ASSETS

These are the digital assets (computerized equipment) that could be affected in the event of a cyber security incident. Threats could be applicable to any of the below listed or similar equipment:

(a) Bridge Systems:
(i) ECDIS, Navigational aids
(ii) GPS, AIS
(iii) VDR
(iv) RADAR
(v) GMDSS equipment
(vi) Weather reporting & routing systems
(vii) Integrated Navigation data reporting systems

(b) Communication Systems:
(i) Inmarsat, Iridium, VSAT & other satellite communication systems
(ii) Wireless communication system
(iii) Email communication PC / systems
(iv) Network Access control servers
(v) File & Email servers
(vi) Antivirus servers
(vii) SSAS

(c) Cargo Systems:
(i) Cargo Load computers

(ii) CCR Console
(iii) Cargo monitoring systems

(d) Propulsion and Machinery:
(i) Engine Control systems
(ii) Alarm Systems and console
(iii) Power Management system
(iv) Real Time data collection systems
(v) Hand-held instruments & data terminals

(e) Access control systems:
(i) Physical access control
(ii) CCTV or other remote monitoring systems
(iii) Remote & access control systems
(iv) Firewalls & Proxy Servers

(f) Crew Welfare Systems:
(i) Crew Communication PC
(ii) Crew communication networks
(iii) Crew network access control system
(iv) BYOD (Bring Your Own Device) like Personal laptops, tablets and phone devices (to use on crew LAN)

6.2. THREAT IDENTIFICATION

(a) Cyber security is not just about preventing hackers gaining access to systems and information systems to prevent losses. Computerized electronic equipments are subject to the usual threats and additionally some unique threats that can be triggered from thousands of miles away, from unseen and unknown intruders or from automatic bots, viruses, worms, etc. which can act either independently or through remote commands.

(b) Detection and containment of such intruders is not only very difficult by also nearly impossible due to the speed of such electronic systems and connections. The best protection is prevention and access control.

(c) Threat from shore-based or shipboard individuals who decide to behave in a malicious or non-malicious manner cannot be ignored and often result in the worst cyber security breaches.

(d) The below lists some of the most prevalent cyber threats:

(i) Triggered from outside
- Hackers, crawlers & bots
- Firewall breaches & Penetration testing
- Phishing email, malicious advertisements
- Malware laden websites
- Breach of password protected assets

(ii) Triggered from inside

i. Password leakage and breaches
ii. Virus and malware infections
iii. Phishing threats, spam and malicious mails
iv. Accessing malicious websites
v. Lack of user training and awareness
vi. Hacked or Pirated software Installations
vii. Document Macros
viii. Deliberate or Malicious actions
ix. Use of Social networks
x. Data loss due to malfunction

(e) Symptoms of computer malfunction:

(i) Computer malfunction symptoms may be exhibited due to varied reasons. It is important to recognize such symptoms and take immediate action are listed below.

(ii) If such actions are not successful, then the symptoms and all relevant information in the form of error messages, screenshots, files or pictures should be sent to the office for further advice or troubleshooting.

No.	Symptoms of malfunction	Actions to be taken
1	Network connectivity issues: This causes Network shortcuts to fail. Programs which rely on network connectivity and resources may not work properly, become unresponsive and web pages may fail to load. Network Shared drives (S:\ drive) may not work or works slowly. MKay lead to data loss.	Check the LAN cables and secure against vibrations. Check and secure power supply of LAN Routers and Switches. If the problem persists, report to office for further advice
2	System Running Slowly: This may be caused by software conflicts, defective hardware, Malware, etc. on the PC which consumes CPU and memory resources in the background.	Reboot the system, run Anti-Virus scan on the system. If problem persists, report to office
3	Inability to boot up on restart: May be caused by corruption of the File System on the boot drive or a hardware error.	Record the boot error and report to office
4	Abnormal noises: Distinct noises such as cooling fans running on high speed, mechanical noises from the computer, beeps and blinking LEDs are usually caused by hardware trouble & failures.	Check ventilation ports for obstructions or dirt. Record the observations in detail and report to office.
5	Random restarts: BSOD (Blue Screen of Death) is the sudden appearance of a blue screen displaying a message that the OS has encountered an error and PC will shut down to prevent damage to the computer. Usually caused by hardware faults or defective software drivers.	Disconnect all hardware from the PC and restart. Take photo of the screen and report to office.
6	Instability and intermittent problems: Caused by Virus infections, Hard disk errors, faulty RAM modules, software conflicts, faulty devices & their	Run Antivirus on the PC and disk error check. Backup all the data to external device. Report to office with relevant information.

	software drivers, power fluctuations and defects, etc.	
7	Display glitches: Displays may blink randomly, show distorted display elements on screen, vertical or horizontal lines and is usually caused by the display adapter or monitor.	Restart the PC, then replace existing monitor. If the problem persists, report the nature of problem.

7. SECURITY PROTOCOLS

7.1. RISK MITIGATION AND RESILIENCE

(a) The below lists the available security mechanisms or mitigation factors available to prevent, combat or recover from a cyber security event, breach or incident.

(b) The use of a particular mitigation factor or recovery procedure will depend on the type and extent of the breach.

7.2. PHYSICAL & LOCAL SECURITY

7.2.1. Access Control

(a) Limiting physical access to devices is the first line of defense to ensure that sensitive assets are not accessible to unauthorized parties.

(b) Access to the vessel and control rooms to be restricted as per vessel security plan.

(c) Third parties should not be allowed unsupervised access to vessel's computerized equipment and their usage to be minimized and monitored for authorized access only.

(d) All data in Shipboard PCs is Company property and this data must never be passed to external parties and must be protected by controlling access to the IT infrastructure to prevent tampering or theft of the data.

(e) All IT infrastructure must be protected against damage and malfunction by suitable measures such as proper securing of the equipment, power supplies, data cables, etc. Special care should be exercised against heavy weather.

7.2.2. Email systems and protection of communications

(a) Email is one of the most important communication tools needed on board vessels. Alternative or secondary Email service implementation may be considered to provide communication continuity in case of failure of the primary mail server due to a cyber security event.

(b) Phishing mails are mails which lure the user into clicking on dubious links or opening potentially unsafe attachments which may harm the computer or steal information or passwords.

(c) Emails often host scams and to avoid data theft, be suspicious of clickbait titles (e.g. offering prizes, advice.)

(d) Due to the potential for security breaches, extreme caution should be exercised in downloading / executing any files attached to email. If the attachment is not clearly business related and/or expected from a known source, it should never be opened or executed.

(e) Check email and names of sender of the message from to ensure they are legitimate. Be aware that you may get a phishing mail from your friend's or contact's infected computer. Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

(f) If there is any doubt that an email received is unsafe, please report it to your PIC or IT Dept. They can check the email forensically and advise you further.

7.2.3. Use of USB ports for storage devices

(a) Sharing of files and other information should be done only via the computer connect to and protected by the business LAN.

(b) In case USB drives need to be used, only USB storage drives provided by the Company are to be used for sharing files. These USB drives should be marked for the purpose and should be scanned by the antivirus every time they are used.

(c) USB Ports on sensitive computerized equipment may be blocked or rendered unusable via software or hardware locks as required. Any breach in such protection should be reported to the IT department.

7.2.4. Antivirus protection (update mechanism, alerts)

(a) All official computers shall always be protected by approved and updated Antivirus program. This will provide protection against malicious code, viruses, worms, etc.

(b) All external devices like USB drives connected to the computers shall be scanned for malicious software by the Antivirus program.

(c) All Computers shall be kept connected to the vessel business LAN to provide various services to the connected computers such as automatic updates for the antivirus software, etc.

(d) The Antivirus programs may also report their status to the AV server and to shore server for effective monitoring of the AV status of the computers.

(e) Any error in the update to the antivirus software shall be promptly reported to the company and rectified earliest possible.

7.2.5. Password protection (operational / administrative)

(a) Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure, so they won't be easily hacked, but they should also remain secret.

(b) All onboard computers shall be password protected to prevent casual access by unauthorized persons.

(c) Computers may be set to automatically lock after a period of inactivity and require a password to gain access again.

(d) Remember passwords instead of writing them down.

(e) Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, you should prefer the phone instead of email.

7.2.6. Software usage

(a) Only Company approved software shall be installed on the vessel computers.

(b) It is prohibited to download or install suspicious, unauthorized, pirated or illegal software on company computers.

(c) Use of such software may lead to fines and penalties by authorities.

(d) The software may have been hacked or modified with malicious intent
   i) To cause instability or conflicts in the IT infrastructure.
   ii) To cause a cyber security breach from inside the vessel network.

(e) Any such software, if found, shall be promptly reported to the IT manager and removed from the computers.

7.2.7. Software data update mechanisms

(a) Equipment and operational systems such as ECDIS, eNP, ADP, AVCS, etc. may be updated via email, Internet or physical media (CD, DVD, USB drive).

(b) Softwares that require periodic data updates shall be kept updated via approved update mechanism as per company or makers' instructions. Various methods such as email, direct internet or CD/DVD may be used as per company instructions.

(c) Software upgrade & version tracking: New versions of software shall be installed as per company instruction via approved update mechanism and from verified sources. Such upgrade of software versions shall be recorded and informed to the company when completed.

(d) Operating system updates: The operating system should be updated via company approved update mechanism either via direct updates over internet or via update CD / DVD. The update shall be carried out for all vessel's computer and confirmed to company for the status.

7.2.8. Remote access and support

(a) Remote access to on board equipment and computerized equipment may be provided to the company or to authorized third parties with express permission from the company.

(b) Firewall rules and passwords for such access to be safeguarded against misuse or theft.

(c) Users may not install personal software designed to provide remote control of the PC or workstation.

(d) This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

7.2.9. Information Backup and redundancy

(a) Sensitive data should be stored / backed up in the network drive.

(b) The network drive should have hardware redundancy for protection against hardware failure of disks and possible auto-backup capability to prevent loss by accidental deletion of data.

7.2.10. Hardware failure & equipment redundancy

(a) Software required for important functions should be installed on more than one computer to ensure continuity in case of failure of the hardware on one machine.

(b) Such software may include PMS, reporting systems, Navigational software such as eNP, ADP, ECDIS update software, etc.

7.2.11. Power supply protection (UPS, Backup power, etc.)

(a) The power supply to important equipment shall be done in a manner such that the equipment function can be restored within a reasonable time after failure of the primary power supply.

(b) Such backups may include use of battery powered computers (Laptops), UPS, Emergency power sources, etc.

7.3. LOCAL AREA NETWORK SECURITY

(a) LAN Separation and VLAN (Virtual LAN):
   (i) Sensitive communication services may be required on the vessel's LAN. Such communication may be kept segregated from the normal LAN services by implementation of physically separate LAN or Virtual LANs.
   (ii) On Internet connected vessels, it is safe to separate the Business use LAN from the Crew use LAN. In such cases, individually configured Firewalls should be used to restrict access and services available for protection of connected assets.

(b) Data sharing over LAN:

(i) Data in the forms of files and streams is transmitted over the LAN to provide sharing and storage functions.

(ii) Access to the LAN connections should be restricted to approved and authorized computerized equipment only and personal or unauthorized computers shall not be connected to the business LAN to prevent unauthorized access to stored data and LAN services.

(c) Network shared (NAS) disks, Backup, redundancy:

(i) Shared data is stored on the shared drive and provides the required access to all computers connected to the LAN for normal functioning of various operational softwares like the PMS, reporting system, etc.

(ii) The Shared drive should be protected against hardware failure (RAID) and possibly against deletion of files and folders, via automatic periodic backup.

(iii) If required, requests for Data recovery shall be made to the company as early as required so that such data can be recovered intact as much as possible.

(d) Connecting Devices to the Network:

(i) Users shall not attach non-company computers that are not authorized, owned and/or controlled by company.

(ii) Only authorized devices may be connected to the Vessel's networks. Authorized devices include PCs and workstations owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

(iii) Swapping or connecting Business LAN computers and devices to the crew LAN is prohibited without express instruction of the IT Dept.

7.4. WIDE AREA NETWORK SECURITY

(a) Firewalls and content filtering:

(i) Firewall provide protection against unwanted and unauthorized access to the vessel part of the WAN & LAN systems.

(ii) All communications systems which can connect to the Internet shall be protected with one or more firewalls.

(iii) Changes to the WAN firewall rules is prohibited without the express approval of the IT Manager.

(b) Content filtering by URL lists (blacklisting by content):
The WAN Firewall should be able to restrict access to categories of websites depending on their categorization and content.

(c) Content blocking by MIME types (.exe, .zip., bat, etc.):
The WAN Firewall should be able to restrict access files depending on the type of content requested.

(d) Allow / Deny access by IP / port:
The WAN Firewall should be able to restrict or allow access to particular websites as per the approval of the company.

(e) Remote Internet access shutdown procedure:

If required, general access to the Internet maybe shutdown on the vessel to maintain minimum communication ability on any of the vessel LANs as deemed necessary by the Company as required due to operational constraints or in the event of a cyber security incident.

(f) Remote access and support:
Remote access to on board assets shall be restricted and such access may be allowed for a limited time for remote troubleshooting. Such access should be password protected and such access should be denied by the firewall.

(g) Remote File transfer:
Any file transmission from / to vessel to shore shall be adequately protected via VPN or similar encryption method to ensure protection and privacy of the data.

8. CYBER SECURITY AND IT POLICY VIOLATION

(a) The company takes the issue of security seriously. Users of the Company technology and information resources must be aware that they can be disciplined if they violate this policy.

(b) Users violating this policy may be subject to disciplinary action up to and including discharge from service. The specific disciplinary penalty imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of the violation.

(c) Many countries are very strict about Copyright issues and pornographic material in shipboard PCs as well as personal laptops or portable hard drives etc. carried by the ship's crew. Such issues may be acceptable in some countries but may be considered a crime in some other countries.

(d) Failure to comply with local regulations can lead to heavy fines and imprisonment.

(e) Company prohibits carrying and storing of pirated software and any pornographic materials in shipboard PCs, drives, Crew personal laptops or portable storage devices, etc.

9. RECOVERY & RESPONSE PLAN

(a) Upon identification of a cyber security incident, the IT manager will initiate a suitable response and investigation for the below
   (i) Identification of cyber security incident
   (ii) Actions subsequent to identification
   (iii) Recovery of systems, data and connectivity
   (iv) Preventive countermeasures

(b) Company recognizes that investigating cyber incidents can be a complex and challenging task. IT Manager, after discussing with top management shall decide which incidents are to be investigated. Industry guidelines on Cyber security shall be referred to under such circumstances.

(c) Company may use external expert assistance to investigate such incidents as appropriate.

Ref:
The guidelines for Cyber Security on Ships – BIMCO/CLIA/ICS/INTERCARGO and INTERTANKO
Code of Practice- Cyber Security for Ships – DOT, UK

9.1. ADDITIONAL & EXPERT ASSISTANCE ACTIVATION FOR RECOVERY

(a) Additional resources may be required and activated for assistance in recovery of normalcy, depending on the severity and extent of the cyber security. Such additional resources may also be called upon to provide expert advice to further improve the protection of the digital assets or to improve resilience and recovery.

(b) Such resources may include the below:
- (i) Company IT Team support
- (ii) Satellite Communication service provider
- (iii) Network control device & software provider.
- (iv) LAN, VLAN & WAN Firewall provider
- (v) Specific Equipment Makers / provider
- (vi) Specific Software makers / provider

10. MODIFICATIONS AND REPAIRS

(a) In order to ensure compatibility and to avoid any conflicts between software and/or network it must be installed by company approved software and computer specialists unless authorized by company.

(b) Any modification should be carried out after obtaining prior consent of the company.

(c) If there is any suggestion for improvement in the software of PCs or the network, the Master should first report the same to the company using IT 01. Company shall consult all such cases with the service provider software company.

(d) In case a problem cannot be corrected by ship staff, the Master shall report the symptoms to the company by using IT 02 (PC Trouble Report) to get assistance for troubleshooting.

(e) The Master shall report to the company on completion of the repairs as instructed. In extreme cases company shall send a technician and / or office staff on board for troubleshooting.

11. MAINTENANCE & CARE OF COMPUTERIZED EQUIPMENT & SYSTEMS

(a) Computerized systems require minimal maintenance to keep operating reliably for a long time. However, general maintenance and good practices are required to be followed diligently in order to ensure maximum reliability and to extend the life of such equipment and systems as per the guidelines laid out earlier in this document.

(b) In addition to carrying out specified PMS tasks, periodic maintenance on computerized systems and equipment may include the below as and when required.

(i) Keeping all plug-in cables, power supplies & equipment secured against ship vibrations.
(ii) Reporting errors & malfunctions in software and hardware for speedy rectification.
(iii) Preventing physical damage to the equipment by proper securing against vessel movement in bad weather and by spill of liquids on the equipment.
(iv) Using original or good quality consumables in equipment such as printers, etc.
(v) Keeping the equipment clean by wiping with soft damp clean cloth. Dust in internal parts & cooling fans should be carefully cleaned with a vacuum cleaner or brush.
(vi) Checking and updating Software and firmware updates, including Antivirus as per company or makers instructions
(vii) Restarting computers periodically to reset malfunctioning programs.

12. CYBER SECURITY ASSESSMENT OF THE VESSELS AND OFFICES

(a) A detailed security assessment shall be done for each vessel and each office annually or after a breach of cyber security incident.

(b) This assessment shall be done for all Information Technology and Operation Technology equipments on each ship and in offices using a checklist IT 03- Cyber Security Assessment Checklist and IT 04- Cyber Security Assessment Checklist(Office). All essential information for each equipment shall be collected and kept in record through this checklist.

(c) IT Team shall take the initiative to rectify Non-Conformities. When the Non-Conformity is severe and, or due to lack of resources, cannot be rectified in three months, Senior Management shall take over the role of taking the initiative to rectify the Non-Conformity.

(d) IT 04- Cyber Security Assessment Checklist(Office) shall be used every year by IT Team for each office and records maintained. Any problems or issues observed during the assessment shall be dealt with as soon as possible.

13. TRAINING REQUIREMENTS

(a) Suitable training for the threats and security protocols as given above to be provided to all seafarers on board in order to mitigate various identified risks to the vessel's Computers and Computerized systems and equipment. Such training should include but not limited to the following:

(i) Sources and Hazards of viruses in ship's computer systems and equipments
(ii) Safeguarding of passwords
(iii) Responsible use of social media
(iv) Use of personal devices, etc.

(b) Above shall be achieved through training program as below:

(i) Upon joining the vessel, each seafarer shall be given Cyber Security familiarization including specific to ship's equipments

(ii) Six monthly training to be provided by senior management to crew onboard. This is be documented in HSSEQ-03 Yearly Training program and HSSEQ-05 Training Record.

(iii) Training should be further enhanced via additional information and training material like posters, videos, incident reports, alerts, software, etc. provided by the company from time to time.

(c) A Cyber Security Awareness poster shall be displayed and / or be used as Screen Saver of PCs at all IT terminals.

App:

IT 01: Change Request for vessel system
IT 02: PC Trouble Report
IT 03: Cyber Security Assessment Checklist
IT 04: Cyber Security Assessment Checklist(Office)

-x-